**Apéndice “A”**

**Coordinación de Telecomunicaciones**

**y Seguridad de la Información**

**Servicios Administrados de Seguridad Informática (SASI) 2025**

**Control de versiones del documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Descripción** | **Responsable** |
| 0.1 | 31/05/2024 | Actualización del Documento | Lic. Cynthia Osmara Verdín Villegas |
| 0.2 | 31/05/2024 | Revisión del Documento | Ing. Abraham Gutierrez Castillo |
| 1.0 | 31/05/2024 | Aprobación del Documento | Lic. Florencio Fernando González Velázquez |
| 1.1 | 13/11/2024 | Ajustes/Revisión del documento | Ing. Abraham Gutiérrez Castillo |
| 2.0 | 20/11/2024 | Aprobación del documento | Ing. Javier Cortes López |

1. Objetivo del Documento

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

2. Servicio de Firewall

Especificaciones Técnicas:

* Cumplir con el desempeño y capacidades considerando al menos las siguientes especificaciones:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Tipo 1** | **Tipo 2** | **Tipo 3** | **Tipo 4** |
| Desempeño | 5 Gbps | 10 Gbps | 20 Gbps | 240 Gbps |
| Conexiones simultaneas por seg. | 1,000,000 | 2,000,000 | 4,000,000 | 32,000,000 |
| Conexiones nuevas por seg. | 50,000 | 125,000 | 200,000 | 1,000,000 |
| Paquetes por seg. | 1,000,000 | 3,000,000 | 5,000,000 | 30,000,000 |
| Interfaces 10GbE | 8 | 8 | 12 | 12 |

* El licitante deberá considerar en su propuesta económica que las características de conexiones simultaneas por segundo se refiere a conexiones concurrentes por segundo.
* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
* Certificado por organismos de la industria como Common Criteria o ICSA Labs.
* Incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
* Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
* Integrar listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.
* Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
* Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
* Capacidad de implementar mecanismos de calidad de servicio tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
* Capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
* Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
* Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
* Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (firewalls virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
* Capacidad de crear hasta 100 instancias de dispositivos virtuales (firewalls virtuales) que deberán ser soportadas en cada uno de los diferentes tipos de firewalls.
* Deberá soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
* Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
* Soportar y operar bajo protocolos de ruteo BGP y OSPF.
* Soportar y operar mediante rutas estáticas.
* Realizar inspección en capa 3 y 4.
* Soporte y operación con al menos 1,000 VLANs
* Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
* Permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
* Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
* Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
* Incluir una consola centralizada de gestión con las siguientes características:
  + Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
  + Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
  + Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
  + Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
  + Agrupación de parámetros de configuración para su posterior implementación.
* Durante una actualización de configuración, deberá ser capaz de regresar a la configuración anterior, si es necesario o requerido.
* Auditoria de todas las actividades realizadas por los usuarios con privilegios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

3. Servicio de Prevención de Intrusos (IPS)

Especificaciones Técnicas:

* Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Tipo 1** | **Tipo 2** | **Tipo 3** | **Tipo 4** |
| Desempeño | 15 Gbps | 20 Gbps | 24 Gbps | 30 Gbps |
| Conexiones simultaneas / concurrentes por seg. | 15,000,000 | 25,000,000 | 30,000,000 | 50,000,000 |
| Conexiones nuevas por seg. | 120,000 | 160,000 | 200,000 | 250,000 |
| Interfaces 10GbE | 4 | 8 | 8 | 8 |

* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Latencia máxima de 0.5 milisegundos.
* Las interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
* Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
* Capacidad de detección en línea sin bloquear tráfico (Modo transparente o supervisión). El sistema sólo alertará que eventos serían bloqueados.
* Capacidad de configuración del modo transparente o supervisión para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo, VLAN ID, entre otros.
* Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
* Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
* Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
* La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
* Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto deberá ser soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
* Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos una vez por mes.
* Soporte de análisis de tráfico de voz sobre IP.
* Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
* Soporte de monitoreo de IPv6.
* Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
* Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
* Detección de escaneo de puertos.
* Detección de re-ensamblaje de paquetes fragmentados.
* Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato. ENC (estándar para el software de análisis de protocolos), dicho archivo podrá ser usado para hacer reconstrucción o análisis forense del ataque.
* Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP “confiables” que el sistema no bloqueará.
* Integración de firmas definidas por el Instituto mediante el uso de expresiones regulares.
* Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
* Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.
* Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
* Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
* Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoría.
* Consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
* Consola remota con interfaz gráfica o Web cifrada (HTTPS) para el uso en modo de consulta, con diferentes perfiles de usuarios.
* Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
* Deberá soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
* Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (IPS virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
* El licitante deberá considerar en su propuesta económica la capacidad de crear hasta 100 instancias de dispositivos virtuales (IPS virtuales) en todos los equipos ofertados.
* Para los equipos en el centro de datos principal se requiere una consola de Administración.

**4. Servicios de Protección contra Denegación (DDoS)**

|  |  |  |
| --- | --- | --- |
|  | **Tipo 1** | **Tipo 2** |
| Desempeño | 20 Gbps | 120 Gbps |
| Conexiones simultaneas por seg. | 25,000,000 | 120,000,000 |
| Conexiones nuevas por seg. | 160,000 | 600,000 |
| Interfaces 10GbE | 8 | 8 |

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* El licitante deberá considerar en su propuesta que la cantidad de tráfico máximo a inspeccionar por lo equipos y un ancho de banda de los enlaces de internet que estarán recibiendo los equipos, de 1 Gbps para ambos casos.
* Deberá garantizar el paso transaccional de datos legítimos, privilegiando la eliminación de tráfico anómalo dentro de los canales de comunicación del Instituto (Clean Pipes).
* Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
* Deberá tener la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
* Deberá de tener capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet/Intranet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en los enlaces.
* Deberá de tener la capacidad de monitoreo en tiempo real las subredes públicas que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
* Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
* Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
* Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
* Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
* Deberá monitorear, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:
  + Para el protocolo IP:
    - ICMP
    - Paquetes IP fragmentados
    - Paquetes IP NULL
    - Paquetes IP con direcciones privadas
  + Para el protocolo TCP:
    - Segmentos TCP NULL
    - Segmentos TCP RST
    - Segmentos SYN
    - Tráfico total
* Deberá como mínimo detectar los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
  + ACK Flood
  + SYN Flood
  + Hogging CPU
  + Chargen (Character generator)
  + FIN Flood
  + ToS Flood
  + DNS Malformed
  + HTTP Flood
  + ICMP Flood
  + UDP Flood
  + Non- UDP/TCP/ICMP Protocol Flood
  + PPS Flood Attack
  + Zombie attack
  + Land Attack
* Deberá de permitir la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
* Deberá monitorear actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
* Deberá monitorear actividad “Dark IP”.
* Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
* Detección de zombis (con selecciones de umbrales en bytes por segundos y paquetes por segundos) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
* Protección contra amenazas conocidas
  + Ping de la muerte
  + Ataque por inundación SYN
  + Fragmentacion de paquetes y reensamblaje
  + Broadcast de correo electrónico
  + Saturadores de CPU
  + Scripts generadores de trafico
  + Generadores de caracteres
  + Ataques fuera de banda (WinNuke)
  + Ataque Smurf (generador de gran cantidad de paquetes ICMP)
* Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
* Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

5. Redes Privadas Virtuales – VPN (C2S – S2S)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Deberá incluir al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
* Deberá tener un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
* Capacidad de permitir 50,000 nuevas conexiones por segundo.
* Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
* Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
* Deberá soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
* Deberá integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
* Deberá permitir la creación de grupos de usuarios.
* Deberá permitir delimitar la cantidad de conexiones por usuarios.
* Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.
* Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
* Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
* Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
* Deberá soportar integridad de datos con md5, sha1 y sha2.
* Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
* Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
* Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
* Deberá realizar VPNs SSL.
* Deberá soportar la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente debe soportar al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.

**6. Filtrado de Contenido Web**

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Soportar de forma mínima 120,000 usuarios de forma simultánea.
* Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
* Permitir operar en modo de proxy explicito y/o proxy transparente.
* Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
* Control de autenticaciones simultáneas con una misma cuenta de usuario.
* Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
* Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
* Catalogar las páginas por dominio (o subdominio), URL o IP.
* Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
* Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
* Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
* Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
* Permitir la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
* Permitir el uso de expresiones regulares.
* Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
* Capacidad de evitar la ejecución de códigos maliciosos.
* Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
* Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
* Permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
* Proporcionar capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
* Deberá proporcionar soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).
* Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

7. Servicios de Filtrado de Contenido de Correo (Antispam)

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Capacidad de hasta 1.5M de correos por hora
* Con una capacidad de por lo menos 120,000 usuarios
* 12 TB por equipo, en HA por lo menos 24 TB.
* Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
* Capacidad de revisar tanto el correo entrante como el saliente.
* Deberá escanear y analizar el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
* Contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos.
* Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP, como en políticas cuando el correo ya ha sido recibido.
* Contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además, se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
* Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
* Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
* Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del fabricante, permitiendo la configuración de umbrales para esta detección.
* Contar con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
* Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
* Contar con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
* Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
* Capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
* Contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen en el dominio destino (correos de rebote o Bounced Mails).
* Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
* Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
* Permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
* Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, podrá realizar cualquiera de las siguientes acciones:
  + Reemplazar texto del mensaje afectado.
  + Poner en cuarentena el mensaje completo.
  + Eliminar el mensaje completo.
  + Hacer copia de seguridad (copia del mensaje), para reportarlo con los centros de investigación de amenazas del fabricante.
* Detectar correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
* Proporcionar la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
* Capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.
* Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

**8. Firewall Especializado en Servicios Web (WAF)**

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

* Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
* Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
* Soportar un throughput de 5 Gbps en capa 7.
* Soportar 100,000 Transacciones por Segundo (TPS).
* El licitante ganador debe considerar en su propuesta en términos de transacciones por segundo de tráfico HTTPS requiriendo PFS/DH (Perfect Forward Secrecy/ Diffie-Hellman) al menos 60,000 tps
* Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
* Detección de ataques por clientes automatizados y robots.
* Detección de URL rewriting u ofuscación del URL.
* Manejo de errores y reescritura de errores para aplicativos Web.
* Capacidad para soportar inspección del protocolo XML.
* Certificado por organismos de la industria como ICSA Labs o PCI.
* Actualización automática de firmas de prevención contra código malicioso.
* Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
* Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
  + SQL injection
  + Cross Site Scripting
  + Cross Site Request Forgery
  + Sensitive Data Exposure
  + Security Misconfiguration
  + Broken Authentication and Session Management
  + Otras nuevas identificadas por OWASP
* Soportar formatos de mensaje:
  + Web 2.0
  + HTML
  + XHML
  + HTML5
  + XML
  + JSON
  + AJAX
  + FLASH
  + JavaScript.
* Soportar Protocolos: TCP v4 y v6, HTTP, HTTPS, SSL/TLS.
* Soportar mitigación de amenazas:
  + HTML Content Aware
  + Intrusion Detection and Prevention (URI patterns)
  + URI rate-based heuristics
  + Vendor Vulnerabilities
  + URL cloaking / rewrite
  + Parameter Inspection
  + Learning mode
* Integridad de transacciones:
  + Session Tracking Cookies, Source/Destination IPs
  + HTTP RFC conformance
  + HTML Form parameter checking
  + Cross-Site Scripting
  + Cookie Signing
* Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
* Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
* Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
* El licitante deberá considerar en su propuesta al menos 200 sitios/portales a proteger.

9. Servicios de Gestión Unificada de Amenazas (UTM)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Tipo 1** | **Tipo 2** | **Tipo 3** | **Tipo 4** |
| Desempeño | 1 Gbps | 2 Gbps | 5 Gbps | 10 Gbps |
| Conexiones simultaneas por seg. | 10,000 | 20,000 | 50,000 | 100,000 |
| Conexiones nuevas por seg. | 150,000 | 500,000 | 1,000,000 | 2,000,000 |
| Interfaces 10/100/1000 Mbps. | 4 | 4 | 8 | 8 |

El licitante deberá considerar en su propuesta que funcionalidad de alta disponibilidad modo Activo/activo y/o Activo/Pasivo.

El licitante deberá considerar en su propuesta que la característica de conexiones simultaneas por segundo” y “conexiones nuevas por segundo, se refiera a conexiones concurrentes por segundo, así como considerar que la suma de las sesiones concurrentes refiere al servicio UTM por cada tipo y las sesiones concurrentes de la tabla de UTM.

Generales

* Deberá incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
* Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall

* Deberá estar basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
* Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
* Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
* Deberá soportar y operar bajo protocolos de ruteo BGP y OSPF.
* Deberá soporte y operar mediante rutas estáticas.
* Deberá realizar inspección en capa 3 y 4.

Funcionalidad IPS e IDS

* Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
* Latencia máxima de 0.5 milisegundos.
* Las interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
* El equipo deberá ser capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado
* Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
* Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
* Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
* Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
* La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
* Reconocimiento de tuneleo de protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
* Detección de re-ensamblaje de paquetes fragmentados.
* integración de listas blanca (IP whitelist) mediante una lista de direcciones IP “confiables” que el sistema no bloqueará.
* Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.

Filtrado de Contenido Web

* Deberá permitir operar en modo de proxy explicito y/o proxy transparente.
* Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL).
* Catalogar las páginas por Dominio (o subdominio), URL o IP.
* Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
* Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
* Capacidad de evitar la ejecución de códigos maliciosos.
* Permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
* Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

Funcionalidad VPN

* Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
* Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
* Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
* Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
* Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
* Deberá soportar integridad de datos con md5, sha1 y sha2.
* Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
* Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
* Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
* Deberá soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).

**10. Firewall Especializado en Base de Datos (DBF)**

Especificaciones Técnicas:

* Tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
* Deberá operar a nivel local y en la capa de red
* Deberá soportar al menos los siguientes motores de Bases de Datos:
  + Microsoft SQL Server
  + Oracle
  + Sybase
  + Informix
  + MySQL
  + Progress
  + PostgreSQL
* Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
* En caso de ser necesario la utilización de agentes, estos deberán soportar al menos los siguientes Sistemas Operativos:
  + AIX
  + HP-UX
  + Solaris
  + RHEL
  + SusE
  + OEL
  + Windows 32/64 bits
* Capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.
* Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
* Se requiere un repositorio para el registro de la actividad, el cual no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
* Capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
* Capacidad para poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
* Capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
* Capacidad para proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
* Deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
* Deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
* Deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
* Deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
* Capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
* Capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
* Deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automática o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
* Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
  + Número de registros a regresar por la consulta (SQL Query)
  + Número de registros afectados
  + Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
  + Acceso a datos marcados como sensibles
  + Base de Datos, Schema, Instancia, Tabla y Columna accesada
  + Estado de autenticación de la sesión
  + Usuario y/o Grupo de Usuarios de Base de Datos conectado
  + Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
  + Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
  + Logins, Logouts, Queries
  + IPs de origen y destino
  + Nombre de Host origen, Usuario firmado en el Host origen
  + Aplicación usada para la conexión a la base de datos
  + Tiempo de respuesta/procesamiento del query
  + Errores en el manejador de SQL
  + Número de ocurrencias en intervalos de tiempo definidos
  + Por operaciones básicas (Select, Insert, Update, Delete)
  + Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
  + Por Stored Procedure o Function utilizada
  + Si existe ticket asignado de cambios
  + Hora del Día
* Deberá posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
* Deberá proteger contra ataques SQL y no-SQL.
* Contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
* Considerar de emergencia, para potenciales violaciones de la información que incluyan, enunciativa más no limitativamente:
  + Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  + Acceso a datos inusual para cierta hora del día.
  + Acceso a datos desde una ubicación (física) desconocida.
  + Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
* Debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
* Debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
* Deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
* Deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de estas.
* Deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
* El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
  + Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
  + Deberá incluir una lista pre-configurada y detallada de las firmas de ataque.
  + Deberá permitir la modificación o adición de firmas por el administrador.
  + Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
  + Deberá detectar ataques conocidos a nivel base de datos
* Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
* Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

11. Servicio de Correlación de Eventos

Especificaciones Técnicas:

* Capacidad para recolectar datos de toda aplicación o dispositivo que tenga una fuente de eventos necesaria para la organización, siendo esto a través de desarrollos predefinidos del fabricante, o con desarrollos personalizados ejecutados por el proveedor del servicio.
* Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo), para efectos de auditoría y análisis forense. La solución deberá generar una firma o “checksum” de los eventos recibidos para garantizar la integridad y mantener la cadena de custodia.
* Permitir la detección automática de fuentes de eventos recolectados a través del protocolo syslog, el cual puede ser enviado vía UDP, TCP o SSL/TLS.
* Capacidad de permitir filtrar eventos por cualquier campo del registro, que son los atributos donde se almacena la información recolectada por la herramienta de las fuentes de eventos.
* Contar con lógica de taxonomía a nivel de la recolección de los eventos, y que permita definir y modificar la misma con base en los eventos auditados.
* Capacidad para detectar automáticamente la desconexión de un conector de integración a través del envío de señales de comunicación para el aseguramiento de la continuidad operativa (“Keep Alive”).
* Capacidad para integrarse con los sistemas de detección y prevención de intrusos y los de administración de vulnerabilidades (VM)
* Contar con la capacidad de emitir notificaciones a partir de eventos y datos recopilados a través de mecanismos como SMTP, SNMP y SYSLOG.
* Correlacionar eventos en tiempo real, es decir, que la información de los eventos sobre los que se está basando deberá venir del flujo del bus de mensajes.
* Capacidad para definir reglas de correlación con distintos niveles de complejidad, partiendo de las basadas en patrones, hasta reglas basadas en periodos de tiempo, anidadas, causa/efecto y secuenciales.
* El módulo de creación de reglas de correlación deberá tener la capacidad de seleccionar eventos para hacer las reglas, así como el seleccionar campos del mismo para ser incluidos en la regla a través de mecanismos como “Drag-and-Drop”.
* Contar con la capacidad de probar las reglas antes de ser implementadas en el motor de correlación.
* Deberá comprimir los datos almacenados al menos con una relación de 10 a 1.
* Contar con mecanismos de monitoreo de la integridad de la información local y archivada.
* Capacidad para soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS o CIFS.
* Contar con una suscripción de boletines de seguridad más importantes del mercado para así identificar las vulnerabilidades conocidas, correlacionando la información de herramientas de administración de vulnerabilidades con los eventos recolectados, lo que permitirá automatizar su detección.
* Se deberán considerar 10,000 eventos por segundo
* Las bitácoras de eventos deberán ser almacenadas por tres meses.

12. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)

Especificaciones Técnicas:

* Detectar cuando un equipo intenta hacer comunicación con un servidor de comando y control en Internet.
* Detectar cuando una amenaza intenta ingresar en la organización mediante internet.
* Detectar e interactuar cuando un atacante o código maliciosos está realizando actividades de movimientos laterales en la organización.
* Detectar ataques del tipo “zero day” que puedan intentar comprometer activos de la organización.
* Tener las capacidades de detección de anomalías en los puntos de la red designados, dicha detección no debe basarse en firmas ni heurística.
* Tener la capacidad de actuar no solo por la generación de alertas de los componentes tecnológicos implementados, si no capacidades de caza de amenazas.
* Contar con las capacidades de análisis y perfilamiento de los actores detrás de un ataque sobre el Instituto.
* Apoyará al Instituto en la detección y prevención de ataques avanzados, así como el manejo de los incidentes que deriven de ello.
* Elevar el nivel de visibilidad respecto a detección de amenazas avanzadas persistentes.
* Elevar el nivel de capacidades de actuación ante una amenaza avanzada persistente.
* Permitir contar con la información suficiente para identificar el impacto real de una amenaza.
* Permitir proteger diversos segmentos de la red del Instituto con diferentes niveles de protección de acuerdo con la criticidad de los usuarios de cada segmento.
* Permitir tener arquitectura modular y escalable de protección y viabilidad.
* Contar con un servicio especializado que permita apoyar al Instituto en la actuación y respuesta ante un ataque desarrollado con amenazas avanzadas.
* Acortar los tiempos de detección y actuación ante una amenaza avanzada.
* Integrar las capacidades de identificar una amenaza cuando tiene comunicación al exterior mediante el servicio de internet del Instituto o movimiento laterales en las diversas localidades, estas capacidades de detección deberán tener la capacidad de perfilar el comportamiento de los usuarios y sus dispositivos con el propósito de detectar cualquier anomalía que puede representar un impacto o riesgo para la Institución
* Disponer de una capa de inteligencia provista por los fabricantes de los componentes tecnológicos y fortalecida por la capa de inteligencia propia del Proveedor; dichas capas deben incluir al menos las siguientes características:
  + IP, URL Maliciosos
  + Hashes de archivos maliciosos
  + Tácticas, técnicas y procedimientos de los atacantes de la región en organizaciones similares al Instituto.
* Proporcionar las capacidades de realizar investigaciones en profundidad para detectar intrusiones que han pasado desapercibidas para los controles de seguridad implementados, esta investigación debe permitir al menos las siguientes capacidades:
  + Caza de amenazas que han estado activas, pero por su comportamiento no han podido ser detectadas.
  + Interacción con el código malicioso y ataques mediante la implementación de trampas en la red y la emulación de servicios.
  + Engaño de los atacantes mediante la implementación de información que pueda rastrear el origen de un ataque.
  + Análisis dinámico de los artefactos detectados.
  + Análisis de indicadores de compromiso en la red de cómputo del Instituto.
* Generar inteligencia accionable con la cual se puedan alimentar los controles preventivos para evitar que una amenaza conocida pueda volver a presentarse o la detección y contención sea temprana.

13. Antivirus

Especificaciones Técnicas:

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

* La solución antivirus debe proteger a los siguientes sistemas operativos, en las plataformas Intel y AMD (Windows Server 2012 y posteriores).
* La solución antivirus deberá integrar agentes para la detección de virus, malware, entre otros en las plataformas de correo electrónico institucional (Exchange Server 2010 y superiores)
* Reputación Web
  + La solución de antivirus deberá contar con un sistema basado en la reputación de sitios web que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.
  + El sistema de reputación de archivos debe estar integrado o desagregado de la consola de antimalware.
  + Niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro o fuera de la red corporativa.
  + Permitir reclasificar sitios web.
  + El sistema de protección Web no deberá depender de ningún explorador en específico.
  + Permitir editar la lista de URL permitidas a nivel general, grupos o personal.
* Ataques de día Zero
  + Cuando es publicada o descubierta una vulnerabilidad en sistema operativo o en alguna aplicación, el Antimalware deberá ser capaz de detener un ataque causado por un malware que aprovecha la vulnerabilidad descubierta.
* Protección Antimalware
  + Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
  + Detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en:
    - Procesos que se ejecutan en la memoria principal (RAM);
    - Archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
    - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
    - Archivos recibidos a través de software de comunicación instantánea (Whatsapp, MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
  + Detectar y proteger a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
  + La detección heurística de virus desconocidos.
* Control de dispositivos
  + Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas.
  + La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.
  + Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir al usuario hacer modificaciones, control total, solo lectura y ejecución, solo lectura en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
* Protección por comportamiento
  + Para aquellos programas que no están permitidos ser ejecutados en la estación de trabajo, deberán ser agregados a una lista de bloqueo de programas específicos.
  + Evitar o monitorear que un programa con comportamiento sospechoso pueda realizar lo siguiente:
    - Duplicar o inyectar archivos de sistema similares.
    - Modificar el archivo de HOST.
    - Incrustar elementos "plugins” en el navegador de Internet Explorer.
    - Instalar librería del programa malicioso.
    - Instale nuevos servicios.
    - Modifique archivos de sistema.
    - Instale servicios o programas para iniciarse al arrancar la estación de trabajo.
* Reporte de amenazas a los laboratorios
  + Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
  + Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.
  + Lanzar una política de seguridad en caso de epidemias.
* Métodos de Actualización, Instalación y desinstalación
  + Instalación de cliente antivirus mediante la URL de la Consola de la solución.
  + Instalación de cliente antivirus mediante línea de comandos o script.
  + Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
  + Lanzamiento de instalación vía integración con el dominio de Active Directory.
  + Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.
  + Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
  + Desinstalación del cliente de forma remota desde la consola de administración.
  + Configuración de Actualizaciones automáticas, así como la fuente de actualización.
  + Distribución de actualizaciones a los clientes de manera Automática y Manual.
  + Actualización de sistema de firmas para clientes sin conectividad al servidor.
  + Actualización de grupo de usuarios por Agentes de Actualización o repositorios.
* Configuración de escaneos
  + Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.
* Privilegios de los usuarios
  + Personalizar los permisos de los clientes para realizar acciones en el software local.
  + Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.
  + Habilitar o deshabilitar opciones para el cliente que frecuentemente entra/sale de la red local.

14. Servicios de Prevención de Perdida de Información

Especificaciones Técnicas:

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

* Presente un Log de auditoría de todas las actividades de los usuarios.
* Proporcione Reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
* Proporcione un mecanismo de alertas y notificaciones.
* Que sea capaz de proporcionar administración basada en roles múltiples con las siguientes opciones:
  + Capacidad para definir roles de usuarios tales como Administrador, administrador de la seguridad o administrador de cuentas.
  + Capacidad para agregar y modificar roles personalizados.
  + Capacidad de configurar cuentas de usuario y asignar un rol particular a cada usuario.
* Tecnología de Detección.
  + Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
  + Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
  + Capacidad de detección basada en expresiones regulares.
  + Capacidad de detección basada en atributos de archivos tales como tipo de archivo y tamaño de archivo.
  + Capacidad de utilizar validación de reglas de expresión.
  + Capaz de extraer y ejecutar escaneo de contenido de documentos dentro de archivos comprimidos tales como archivos zip y rar.
  + Capaz de controlar la cantidad de capas de compresión que va a descomprimir en archivos comprimidos.
  + Capaz de soportar texto en diferentes idiomas (al menos español e inglés).
  + Que sea capaz de definir identificadores de datos a través de palabras, expresiones o atributos de archivos.
  + Proporcione identificadores de datos predefinidos.
  + Capaz de duplicar y personalizar identificadores de datos predefinidos y personalizados.
  + Capaz de crear identificadores de datos múltiples.
  + Que sea capaz de combinar palabras, expresiones y atributos de archivos dentro de plantillas para identificar información sensible.
  + Proporcione plantillas predefinidas.
  + Con capacidad para importar y exportar plantillas.
  + Capacidad para crear diversas plantillas personalizadas.
  + Capaz de combinar diversas plantillas dentro de una política.
  + Capacidad de crear diversas políticas.
  + Capacidad de crear políticas desde la consola de administración centralizada.
  + Capaz de soportar diversas acciones para una política simple.
  + Capaz de definir un set diferente de acciones basado en la condición de la máquina si está dentro o fuera de la red.
  + Capaz de soportar las siguientes acciones cuando haya fuga de información sensible:
    - Sólo registro del evento (Log violation only).
    - Bloqueo de la transferencia de datos (Block data transfer).
    - Alertas en el equipo del cliente (Client-side alerts).
    - Alertas en el servidor de DLP (Server-side alerting).
    - Almacenamiento de información para análisis forense (Forensic data-capture)
* Debe de ser capaz de ejecutar escaneos de contenido en los siguientes canales de información:
  + Correo electrónico
  + HTTP/HTTPS
  + FTP
  + Dispositivos removibles
  + Copia de información a CD/DVD
  + Mensajería instantánea
  + Comando de impresión
  + P2P
  + Portapapeles
  + Correo web
* Capaz de restringir acceso a los siguientes dispositivos:
  + Unidades extraíbles
  + Unidades ópticas
  + IEEE 1394
  + Impresión de pantalla
  + Bluetooth
  + Tarjetas PCMCIA
  + Carpetas compartidas
* Capaz de especificar excepciones de dispositivos
  + Capaz de definir diversas excepciones.
  + Capaz de utilizar comodines cuando se defina una excepción de dispositivos.
  + La configuración de control de dispositivos se debe de realizar de forma centralizada, desde la consola de administración.
  + Capaz de enviar un mensaje de notificación en la computadora del cliente.
  + Capaz de guardar en el log los eventos de control de dispositivos.

15. Generales para todas las soluciones

* Todas las soluciones deben de cumplir como mínimo con estas especificaciones y capacidades, lo cual son enunciativas más no limitativas.
* Las propuestas deberán considerar todos los componentes necesarios para su correcta operación (Equipo activo de Telecomunicaciones, cableado, módulos, etc.)
* Las propuestas Técnicas, deberán ser acompañadas de las hojas de especificaciones, trípticos y demás información que permita verificar el cumplimiento de las mismas.
* Los proveedores podrán realizar propuestas de mejora de cada una de las soluciones y/o diseño de la red con forme a sus propuestas.
* De las propuestas de solución, podrán proponer arreglos tipo cluster.

**16. Especificaciones físicas y estándares de conexión para los insumos que conforman los Servicios Administrados de Seguridad Informática 2025**

* Especificación y requerimientos de energía eléctrica

El Instituto proporcionará las facilidades dentro de los centros de datos para la alimentación eléctrica (contactos regulados), para el funcionamiento y operación del equipamiento propuesto por el licitante, el proveedor deberá considerar en su propuesta técnica la característica, cantidad, ubicación y los tipos de contactos requeridos para el aprovisionamiento inicial.

* Especificación y requerimientos de espacio físico y ambiental

El Instituto proporcionará la información específica respecto al espacio físico asignado para que el proveedor adjudicado instale la infraestructura de redes y seguridad en los centros de datos correspondientes. Para tal efecto el licitante deberá incluir en su propuesta técnica un apartado indicando la cantidad de espacio físico mínimo indispensable que se requerirá para la instalación de la infraestructura de seguridad.

También se deberá contar con las facilidades para su instalación y se deberá apegar al reglamento y políticas internas para la instalación dentro de cada Centro de Datos. Así también deberá indicar las condiciones ambientales adecuadas para el funcionamiento del equipo a instalar para dar el servicio.

* Especificación y requerimiento para el montaje de hardware

Debido a que el requerimiento del Instituto es un servicio administrado, será responsabilidad del proveedor adjudicado el montaje de los equipos propuestos, racks, gabinetes, rack de panel de parcheo (Parch panel rack), distribuidores fibra óptica, y todo lo necesario para la correcta operación de la solución propuesta, por lo que, en su propuesta económica debe considerar todo lo necesario con la finalidad de proveer lo necesario.

* Especificación para racks

El proveedor adjudicado deberá cumplir con las especificaciones de los racks y gabinetes, incluyendo sus dimensiones físicas, para cada uno de los centros de datos donde el Instituto indique para implementar los Servicios SASI 2025, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto.

* Políticas de cableado estructurado en centro de datos

El proveedor adjudicado deberá cumplir con los requerimientos para cada uno de los Centros de Datos donde el Instituto indique implementar los Servicios SASI 2025, y en apego a las normas y estándares de la industria y los que se acuerdan o indiquen durante las mesas de trabajo con el Instituto, así mismo el proveedor adjudicado deberá suministrar los elementos para la interconectividad necesarios, por lo que deberá: proporcionar e implementar los distribuidores de fibras, las canaletas, los jumpers, y cualquier otro elemento que sea necesario para la correcta interconexión de los racks o puntos de interconexión bajo los estándares de cableado estructurado.

* Especificación de cableado para racks

El licitante deberá contemplar dentro de su propuesta (tanto para el aprovisionamiento inicial, como durante la operación y vigencia del contrato), todo el cableado, jumpers y patch cords necesarios para lograr la interconexión propuesta de todos y cada uno de los módulos y elementos del sistema.

* Especificaciones y requerimientos técnicos de cableado y conectores

Todos los componentes del sistema de cableado, así como troncales de cobre y/o fibra –excepto los correspondientes a los servidores- necesarios para la interconexión de todos los módulos de hardware solicitados para suministrar el servicio de SASI 2025 en el Centro de Datos deberán incluirse como parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.

* Especificaciones y requerimientos técnicos de equipo de comunicaciones de red

Todos los componentes de interconexión (comunicaciones o balanceo de cargas) que apoyen la operación y administración que se lleve a cabo entre las soluciones de seguridad y red, que por su naturaleza sean requeridos para la puesta en operación del servicio de SASI 2025 en el Centro de Datos, deberán incluirse como parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.

* Políticas de seguridad de acceso físico a externos

El proveedor adjudicado deberá cumplir las políticas de seguridad de acceso físico a externos en los centros de datos donde el instituto determine para la provisión de los Servicios correspondientes SASI 2025.

* Especificación y requerimientos de sistema de canalización.

El proveedor adjudicado deberá salvaguardar la integridad física del cableado para evitar fallas potenciales en la operación. De este modo, para salvaguardar la correcta operación del sistema de cableado de fibra óptica y cableado UTP, el licitante ganador utilizará la infraestructura existente en los Centros de Datos y, en general, cumplirá con las norma y políticas de canalización en los mencionados Centros de Datos.

**17. Condiciones para los servicios de mantenimiento**

El proveedor adjudicado será responsable de realizar las tareas de mantenimiento preventivo y correctivo para la totalidad de la infraestructura dentro del alcance de los servicios de SASI 2025, a través de las labores que considere necesarias y de acuerdo con la estrategia de entrega y soporte de los servicios correspondientes. Enseguida se detallan las condiciones específicas para este servicio.

**18. Condiciones para los servicios de mantenimiento preventivo**

Como parte del Servicio de Mantenimiento el proveedor adjudicado deberá realizar al menos un mantenimiento preventivo al año a toda la infraestructura que forme parte del contrato de SASI 2025. Para lo cual deberá integrar un Plan de Mantenimiento Preventivo, en el cual debe tomar en cuenta para la proyección de mantenimientos, las ventanas de mantenimiento necesarias, con el fin de ser programadas e informadas con anticipación al administrador del contrato, con objeto de minimizar el impacto a la operación.

En la correspondiente propuesta técnica el licitante, deberá incluir un Plan de Mantenimiento Preventivo, el cual deberá incluir como mínimo:

* La descripción de los procesos asociados.
* Los Recursos Humanos y Materiales involucrados.
* Los alcances técnicos del mantenimiento y los protocolos de prueba.
* Las rutas de escalamiento correspondientes.

Esta información debe agruparse por tipo de equipo o infraestructura. Para cada caso, el proveedor adjudicado deberá contemplar el calendario de los servicios de mantenimiento preventivo, el cual será validado y autorizado por administrador del contrato, quien revisará que no afecte períodos críticos de la operación del Instituto.

El calendario final de mantenimientos preventivos, fundamentado en el Plan de Mantenimiento Preventivo que se entregará durante las Mesas de Trabajo, será elaborado por El licitante ganador y autorizado por el Instituto, acotando los inmuebles, fechas y actividades a realizar con el máximo detalle, a efectos de coordinar todas las labores necesarias para su correcta ejecución.

**19. Condiciones para los servicios de mantenimiento correctivo**

El proveedor adjudicado será responsable de realizar el mantenimiento correctivo para los servicios correspondientes de SASI 2022-2024, para lo cual, previamente deberá integrar a su propuesta los procedimientos para reportar un incidente que requiera mantenimiento correctivo, y un ejemplo de matriz de escalamiento con los niveles y tiempos establecidos entre cada nivel.

Como parte de las Mesas de Trabajo, El licitante ganador deberá proporcionar la Matriz de Escalamiento con los nombres de contactos y responsables.

El licitante ganador efectuará el servicio de Mantenimiento Correctivo cuantas veces sea necesario durante la vigencia del servicio, de acuerdo con las especificaciones técnicas del fabricante y consistirá en la reparación o remplazo de las partes dañadas del equipo, cuando ocurra una falla que así lo requiera.

Si el equipo en cuestión no puede ser reparado, deberá sustituirse por otro equipo de características técnicas iguales o superiores, sin que esto implique la degradación del nivel de servicio requerido para dicho equipo. El tiempo para el reemplazo de partes no deberá exceder los 30 días naturales, durante los cuales El licitante ganador deberá proporcionar un equipo provisional para mantener la operación. El tiempo para el reemplazo de equipos no deberá exceder los 45 días naturales, durante los cuales el licitante ganador deberá proporcionar un equipo provisional para mantener la operación.

**20. Firmas de elaboración, revisión y aprobación**

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaboró/Revisó** | **Cargo** | **Firma** | **Fecha** |
|  |  |  | 13/11/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Aprobó** | **Cargo** | **Firma** | **Fecha** |
|  |  |  | 20/11/2024 |